

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

DAVID SGRO, on behalf of himself and all others
similarly situated,

Plaintiff,

v.

APPLE INC.,

Defendant.

Case No.

COMPLAINT -- CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiff David Sgro (“Plaintiff”), on behalf of himself and all others similarly situated, brings this class action suit for damages and equitable relief against Defendant Apple Inc. (“Defendant” or “Apple”) and alleges the following based upon personal information as to allegations regarding himself and the investigation of his counsel, and on information and belief as to all other allegations:

NATURE OF THE ACTION

1. This is an action brought on behalf of a class of consumers to seek redress for Apple’s systematic violations of state wiretapping, privacy, and consumer fraud laws.

2. This case relates to a flagrant violation of consumer privacy. Quite simply, Apple unlawfully records and uses consumers’ personal information and activity on its consumer mobile devices and applications (“apps”), even after consumers explicitly indicate through Apple’s mobile device settings that they do not want their data and information shared. This activity amounts to an enormous wealth of data that Apple collects and uses for its financial gain.

3. Consumers care about keeping their data private and are demanding more control over their data. Consumers are also becoming increasingly concerned that their private information is being used without their knowledge or permission.

4. As privacy concerns have grown, Apple has sought to position itself as a leader by touting how its mobile devices allow users to control the information they share. For example, the “Apple Privacy Policy” states:

At Apple, we respect your ability to know, access, correct, transfer, ***restrict the processing of***, and delete your personal data.¹

(emphasis added).

5. The Apple App Store “User Privacy and Data Use” page similarly declares:

The App Store is designed to be a safe and trusted place for users to discover apps created by talented developers around the world. Apps on the App Store are held to ***a high standard for privacy***, security, and content because ***nothing is more important than maintaining users’ trust***.²

(emphasis added).

6. Apple even provides specific instructions to users to explain how to control what data Apple collects. Apple tells users to turn off “Allow Apps to Request to Track” in their device settings if they so wish.

7. In addition, Apple makes an outright promise in its mobile devices’ settings: Apple states that it will “disable [the sharing of] Device Analytics altogether” if a consumer toggles or

¹ <https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-en-ww.pdf> (last updated December 22, 2022).

² <https://developer.apple.com/app-store/user-privacy-and-data-use/>.

turns off “Share iPhone Analytics,” on an iPhone, or similar settings on other Apple mobile devices, like the iPad.³

8. Yet, Apple does not honor users’ requests to restrict data sharing.

9. A recent test performed by two independent app developers at the software company Mysk revealed that even when consumers actively change their “privacy settings” and follows Apple’s instructions to protect their privacy, Apple still records, tracks, collects, and monetizes consumers’ analytics data, including browsing history and activity information. These experts and their testing further showed that Apple continues to access consumers’ app usage, app browsing communications, and personal information in its proprietary apps, including the App Store, Apple Music, Apple TV, Books, and Stocks, even when consumers have affirmatively turned off “Allow Apps to Request to Track” and/or “Share [Device] Analytics” on their privacy controls.

10. *Gizmodo* broke the story on the issue on November 8, 2022.⁴ The issue has been reported in multiple news outlets since *Gizmodo*’s report, including *The Verge*, *Engadget*, and *Fox News*.⁵

³ If a consumer has an Apple Watch paired to their iPhone, they must instead turn off the setting for “Share iPhone and Watch analytics” for the same effect. Hereinafter, this setting, across devices, will be referred to as “Share [Device] Analytics.”

⁴ <https://gizmodo.com/apple-iphone-analytics-tracking-even-when-off-app-store-1849757558>.

⁵ <https://www.theverge.com/2022/11/21/23471827/apple-app-store-data-collection-analytics-personal-info-privacy>; <https://www.engadget.com/apple-phone-usage-data-not-anonymous-researchers-185334975>; [html; https://www.foxnews.com/tech/apple-iphone-data-not-as-anonymous-company-says-researchers](https://www.foxnews.com/tech/apple-iphone-data-not-as-anonymous-company-says-researchers).

11. Apple's practices deceive consumers and its collection of data of users who have specifically followed Apple's instructions to prevent sharing of its data constitute an unlawful interception of a communication and violate, *inter alia*, Pennsylvania's wiretapping laws.

12. Plaintiff is an individual whose mobile app usage was tracked by Apple after affirmatively electing to turn off the "Allow Apps to Request to Track" and/or "Share [Device] Analytics" options.

13. Apple, through its tracking and hoarding of data, collected and monetized consumer information without Plaintiff and similarly situated consumers' consent.

14. Plaintiff seeks damages and equitable relief on behalf of himself and all other similarly situated Apple device users in Pennsylvania (the "Class"), arising from Apple's knowing and unauthorized copying, taking, use, and tracking of consumers' communications and activity, and its knowing and unauthorized invasion of consumer privacy.

THE PARTIES

15. Plaintiff David Sgro is a resident of Quakertown, Pennsylvania and a citizen of Pennsylvania. He has an iPhone SE. Until approximately October 2022, Plaintiff Sgro regularly accessed iPhone apps including the App Store, Maps, and Weather. On the same day that Plaintiff Sgro purchased the phone, he turned off the "Allow Apps to Request to Track," the "Personalized Ads" and "Share iPhone Analytics" options. Apple has nevertheless accessed his data while these features were turned off.

16. Defendant Apple Inc. is incorporated in California and maintains its principal place of business at One Apple Park Way, Cupertino, CA 95014.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the aggregate amount in controversy exceeds \$5 million,

exclusive of interests and costs; more than 100 class members are involved; and members of the proposed Class are citizens of a different state (Pennsylvania) than the Defendant (California).

18. This Court has personal jurisdiction over Defendant Apple because Defendant committed the tortious acts alleged herein in Pennsylvania, regularly conducts business in this District, has extensive contacts with this forum, and because a substantial part of the events or omissions giving rise to the claims asserted occurred in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in this District, Defendant transacts substantial business in this District, and Plaintiff resides in this district.

20. This Court has supplemental jurisdiction over the state law claims, pursuant to 28 U.S.C. § 1367.

FACTUAL ALLEGATIONS

A. Consumers have a reasonable expectation of privacy on their mobile devices.

21. More than 1 billion consumers currently use iPhones, and over 1.9 billion iPhones have been sold. Apple's iPhones make up over 23% of the global market share for smart phones.

22. Mobile device users reasonably expect their activity will not be shared without affirmative consent.

23. Tellingly, when Apple announced its iPhone operating system update in 2021 (i.e., iOS 15.2), it introduced App Tracking Transparency, purportedly requiring all app developers to ask users for affirmative consent before tracking their activity through third-party apps and

websites.⁶ In the United States, 94% of users said no.⁷ “[W]hen given the choice, people would rather not be tracked.”⁸

24. Apple has attempted to differentiate itself from its competitors by playing up its commitment to privacy. Recently Apple launched a world-wide ad campaign, erecting 40-foot billboards featuring the iPhone and a simple slogan, “Privacy. That’s iPhone.”⁹



⁶ Jason Aten, *Apple’s iOS 15.2 Is a Major Privacy Update That Lets You See How Apps Are Tracking You. It’s Very Bad News for Facebook, Inc.* (Dec. 14, 2021), <https://www.inc.com/jason-aten/apples-ios-152-is-a-major-privacy-update-that-lets-you-see-how-apps-are-tracking-you-its-very-bad-news-for-facebook.html>.

⁷ Rachel Kraus, *After update, only 4 percent of iOS users in U.S. let apps track them*, Mashable (May 7, 2021), <https://mashable.com/article/ios-14-5-users-opt-out-of-ad-tracking>.

⁸ *Id.*

⁹ *Apple and Privacy*, Apple Insider, <https://appleinsider.com/inside/apple-and-privacy>.

25. Other billboards are similarly plastered with Apple's purported commitment to privacy. "What happens on your iPhone, stays on your iPhone," announced one billboard in Las Vegas.¹⁰ "Your iPhone knows a lot about you. But we don't," announced another in New York.¹¹



26. In one Apple video advertisement in the same privacy campaign, a consumer stumbles upon a "data auction" as the auctioneer pretends to offer up the various data that apps have collected about the consumer. "Her location data," the auctioneer says as a map is placed on

¹⁰ Hamza Shaban, *Apple stars at giant tech confab CES — without actually being there*, Washington Post (January 7, 2019) [https://www.washingtonpost.com/technology/2019/01/07/apple-burns-google-giant-billboard-touting-privacy-ces.](https://www.washingtonpost.com/technology/2019/01/07/apple-burns-google-giant-billboard-touting-privacy-ces/)

¹¹ <https://www.alamy.com/a-billboard-on-the-side-of-a-building-in-midtown-manchattan-on-tuesday-july-9-2019-informs-viewers-of-the-privacy-afforded-by-using-apple-devices-richard-b-levine-image260045682.html>.

the block and offered to the audience. “It’s not data, it’s commerce! Do I hear 600? 620?” At the end, text on the screen says, “It’s your data. iPhone helps keep it that way.”¹²

27. In another Apple advertisement, the narrator says, “Your information is for sale. You have become the product.” After introducing Apple’s privacy options, the narrator says, “Whatever you choose is up to you... App Tracking Transparency. A simple new feature that puts your data back in your control.”¹³

28. More broadly, consumers are worried about their privacy online. According to Cisco, 86% of consumers say they care about data privacy and want more control over their data.¹⁴ Nearly half of those surveyed said they felt unable to protect their personal data—mainly because companies are not transparent about how they use consumer data.¹⁵ A study by Pew Research Center showed that 79% of Americans are concerned about the way their data is being used by companies.¹⁶

29. Industry observers have introduced the concept of “surveillance capitalism,” speaking to “consumers’ increasing awareness that their data is bought, sold, and used without their consent—and their growing reluctance to put up with it.”

¹² <https://youtu.be/NOXK4EVFmJY>.

¹³ https://youtu.be/Ihw_Al4RNno.

¹⁴ *Consumer Privacy Study: Building Consumer Confidence Through Transparency and Control*, Cisco (Sept. 29, 2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf.

¹⁵ *Id.*

¹⁶ *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information>.

30. In sum, while consumer data becomes more valuable to businesses, consumers are becoming more protective about businesses obtaining that data.¹⁷

B. Apple secretly collects consumers’ personal information and tracks their mobile device and app activity.

31. Apple surreptitiously tracks a wide range of consumer activity.

32. Consumer “actions” that Defendant tracks include: (a) how a user initially found an app; (b) the duration a user looked at an app in the app store; (b) the user’s searches in the app store; (c) the advertisements displayed to each user, and (d) which apps the users clicked on.

33. Not only does the App Store send to Apple this individualized information about users’ activities, it also shares the types of phone used, and even screen resolution and keyboard settings.

34. Apple is also able to track user activity across its various apps, as the data analytics it collects share user ID numbers.

35. For instance, Apple “Stocks” shares a user’s private information relating to a user’s investment activities or preferences. It shares with Apple which stock the user is following or viewing. Apple even collects time-stamps on when the user is viewing certain stocks and engaging with the Stocks app.

36. In addition, Apple collects the news articles that users see within their mobile device.

37. Despite branding its products as designed to respect and protect users’ privacy, Apple ignores users’ expressed preferences to keep their data private for their own profit. Apple

¹⁷ Hossein Rahnama & Alex “Sandy” Pentland, *The New Rules of Data Privacy*, Harvard Business Review (Feb. 25, 2022), <https://hbr.org/2022/02/the-new-rules-of-data-privacy>.

misappropriates users' information to make its advertising algorithms more effective, which in turn, generates Apple more revenue from advertisers.

38. In short, Apple cannot justify collecting private user data when users expressly direct Apple not to do so by turning off "Allow Apps to Request to Track" and/or "Share [Device] Analytics."

39. Apple has not disclosed to users that it was continuing to track their private data, in direct contravention of the users' requests that Apple not do so, using the very steps Apple instructs users to stop data collection.

40. Because of Apple's deception and knowing concealment, any applicable statute of limitations has been tolled until only recently, when Plaintiff discovered his data was being tracked.

CLASS ACTION ALLEGATIONS

41. Plaintiff brings this action on behalf of himself and on behalf of the following proposed class:

All individuals who, while using an Apple mobile device in Pennsylvania, had their information tracked or intercepted by Apple after turning off "Allow Apps to Request to Track," "Share iPhone Analytics" and/or any other similar setting on an Apple mobile device that purported to stop Apple from collecting mobile app activity.

42. Excluded from the proposed Class are Apple, its parents, subsidiaries, affiliates, officers, and directors, any entity in which Apple has a controlling interest.

43. Plaintiff reserves the right to re-define any of the class definitions prior to class certification and after having the opportunity to conduct discovery.

44. The claims of all class members derive directly from a single course of conduct by Apple. Apple has engaged and continues to engage in uniform and standardized conduct toward the putative class members.

45. Certification of Plaintiff's claims is appropriate because the elements of each of Plaintiff's claims can be proven (or disproven) on a class-wide basis using the common evidence.

46. Accordingly, Plaintiff brings this lawsuit as a class action on Plaintiff's own behalf and on behalf of all other business, entities, and individuals similarly situated pursuant to Fed. R. Civ. P. 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 23.

47. **Numerosity** (Fed. R. Civ. P. 23(a)(1)). The members of the proposed Class are so numerous that their individual joinder would be impracticable. While the exact number is not known at this time, it is generally ascertainable by appropriate discovery, and it is believed that the Class includes many hundreds of thousands of members, if not more. The precise number of class members, and their addresses, are unknown to Plaintiff at this time but can be ascertained from Defendant's records.

48. **Commonality and Predominance** (Fed. R. Civ. P. 23(a)(2); 23(b)(3)). Common questions of law and fact exist as to all class members. These questions predominate over the questions affecting only individual class members. The common legal and factual questions include, without limitation:

- (a) whether Defendant collected or tracked mobile user information and data without the class members' consent;

- (b) whether Defendant intercepted Plaintiff and the class members' communications within the meaning of Pennsylvania's Wiretapping and Electronic Surveillance Act;
- (c) whether Plaintiff and the Class are entitled to actual, compensatory, nominal, statutory, enhanced, and/or punitive damages, and if so in what amount; and
- (d) whether Plaintiff and the Class are entitled to injunctive, declaratory relief, or other equitable relief.

49. **Typicality of Claims** (Fed. R. Civ. P. 23(a)(3)). The claims of the Plaintiff and the putative class members are based on the same legal theories and arise from the same unlawful and willful conduct of Defendant, resulting in the same injury to the Plaintiff and the class members. Plaintiff and all class members are similarly affected by Defendant's wrongful conduct, were damaged in the same way, and seek the same relief. Plaintiff's interests coincide with, and are not antagonistic to, those of the other class members. Plaintiff has been damaged by the same wrongdoing set forth in this Complaint.

50. **Adequacy of Representation** (Fed. R. Civ. P. 23(a)(4)). Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the class members, and he has retained counsel competent and experienced in complex class action, business competition, and consumer privacy litigation. Plaintiff and his counsel will fairly and adequately protect the interest of the class members.

51. **Superiority of a Class Action** (Fed. R. Civ. P. 23(b)(3)). A class action is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and class members. There is no special interest in class members individually controlling the prosecution of

separate actions. The damages suffered by individual class members, while significant, are small given the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. Further, it would be virtually impossible for the class members individually to redress effectively the wrongs done to them. And, even if class members themselves could afford such individual litigation; the court system could not, given the thousands or even millions of cases that would need to be filed. Individualized litigation would also present a potential for inconsistent or contradictory judgments. Individualized litigation would increase the delay and expense to all parties and the court system, given the complex legal and factual issues involved. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

52. Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)). In the alternative, this action may properly be maintained as a class action, because:

(a) the prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudication with respect to individual class members, which would establish incompatible standards of conduct for Defendant; or

(b) the prosecution of separate actions by individual class members would create a risk of adjudications with respect to individual class members which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect

to the Class as a whole.

FIRST CAUSE OF ACTION

**Violation of Pennsylvania’s Wiretapping and Electronic Surveillance Act (“WESCA”)
18 Pa. Cons. Stat. § 5701, *et. seq.*
(On Behalf of Plaintiff and the Class)**

53. Plaintiff incorporates by reference all allegations in this Complaint and restates them as if fully set forth herein.

54. The Pennsylvania Wiretapping and Electronic Surveillance Act (“WESCA”) prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

55. Any person who intercepts, discloses or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the WESCA is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys’ fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

56. “Intercept” is defined as any “[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.” 18 Pa. Cons. Stat. § 5702.

57. “Contents” when “used with respect to any wire, electronic or oral communication,” is defined as “any information concerning the substance, purport, or meaning of that communication.” 18 Pa. Cons. Stat. § 5702.

58. “Person” is defined as “any individual, partnership, association, joint stock company, trust or corporation.” 18 Pa. Cons. Stat. § 5702.

59. “Electronic communication” is defined as “[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.” 18 Pa. Cons. Stat. § 5702.

60. Apple is a person for the purposes of the WESCA because it is a corporation.

61. Apple’s mobile devices are a “device” used for the acquisition of the contents of any wire, electronic, or oral communication within the meaning of the WESCA.

62. Plaintiff’s and Class members’ intercepted personal information and consumer data constitute the “contents” of “electronic communication[s]” within the meaning of the WESCA. *See Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 132 (3d Cir. 2022). There is no direct-party exception to WESCA. *See id.* at 129 & n.5.

63. Defendant intentionally intercepts and procures Plaintiff’s personal information without consent, even when the “Allow Apps to Request to Track” and/or “Share [Device] Analytics” settings are turned off.

64. Plaintiff’s and Class members’ electronic communications are intercepted contemporaneously with their transmission.

65. Plaintiff and Class members did not consent to having their personal information wiretapped.

66. Pursuant to 18 Pa. Cons. Stat. § 5725(a), Plaintiff and the Class members seek (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys’ fees and other litigation costs incurred.

67. As the Third Circuit recently stated in *Popa*, the WESCA’s use of the term intercept “reduces to acquiring certain communications using a device. And based on just that definition, anyone could ‘intercept’ communications, including people who ‘acquire’ a text message or chat sent directly to them.” 52 F.4th at 126. The court held, “Consistent with [WESCA’s] emphasis [on the protection of privacy], it applies when anyone intercepts communications—that is, takes an action to acquire them with a device. And it requires all parties—not just *a* party—to consent to that interception.” *Id.* at 133. The court further made clear that “there is no sweeping direct-party exception to civil liability under the WESCA.” *Id.* at 129 & n.5.

68. This holding was confirmed when the court denied the petition for rehearing en banc, on October 18, 2022. To avoid running afoul of the WESCA, the Third Circuit identified a simple solution: obtain consent. Here, Defendant did not obtain consent before intercepting the communications of Plaintiff and the Class members.

69. Defendant’s conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members without their consent any time Plaintiff and Class members interact with Defendant’s apps. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

SECOND CAUSE OF ACTION

Violation of Pennsylvania Unfair Trade Practices and Consumer Protection Law

**73 Pa. Stat. Ann. § 201-3
(On Behalf of Plaintiff and the Class)**

70. Plaintiff incorporates by reference all allegations in this Complaint and restates them as if fully set forth herein.

71. The Pennsylvania Unfair Trade Practices and Consumer Protection Law (“UTPCPL”) prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce” 73 Pa. Stat. Ann. § 201-3.

72. Defendant’s design, manufacture, distribution, marketing, advertising, labeling, and sale of mobile devices constitutes “trade and commerce” under 73 Pa. Stat. Ann. § 201-2(3).

73. Defendant violated the UTPCPL by representing that its mobile devices enable users to choose settings that would stop Defendant from collecting or tracking their private data—a feature they do not have (73 Pa. Stat. Ann. § 201-2(4)(v)); failing to comply with the terms of a written guarantee or warranty given to the buyer (73 Pa. Stat. Ann. § 201-2(4)(xiv)); and engaging in deceptive conduct which creates a likelihood of confusion or misunderstanding about privacy settings on Defendant’s mobile devices.

74. Defendant’s deceptive acts and practices, and misrepresentations and omissions, have deceived Plaintiff, and those same business practices have deceived or are likely to deceive members of the consuming public and the other members of the Class.

75. As a direct and proximate result of Defendant’s acts and practices, Plaintiff and the other Pennsylvania Class members have suffered ascertainable loss and actual damages.

THIRD CAUSE OF ACTION

**Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)**

76. Plaintiff incorporates by reference all allegations in this Complaint and restates them as if fully set forth herein.

77. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania Constitution.

78. Plaintiff and class members have an objective, reasonable expectation of privacy in their personal information.

79. Plaintiff and class members did not consent to, authorize, or know about Defendant's intrusion into their mobile devices and apps. Plaintiff and Class members never agreed that Defendant could collect their personal information.

80. Plaintiff and class members had an objective interest in precluding the collection and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

81. Defendant intentionally intrudes on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

82. Defendant's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

83. Plaintiff and Class members were harmed by Defendant's wrongful conduct. Defendant's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

84. Defendant's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their mobile device and app activity. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

85. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's mobile device and apps, without providing proper consideration for Plaintiff's and Class member's property.

86. Further, Defendant has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

87. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

88. Defendant's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members without their consent any time Plaintiff and Class members interact with Defendant's apps. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

FOURTH CAUSE OF ACTION

Breach of Implied Contract **(On Behalf of Plaintiff and the Class)**

89. Plaintiff incorporates by reference all allegations in this Complaint and restates them as if fully set forth herein.

90. Plaintiff and Apple entered into a contract for the sale of an Apple mobile device.

91. As part of that agreement, and by providing consumers with the ability to turn off the “Allow Apps to Request to Track,” “Share iPhone Analytics” and similar settings, Apple impliedly promised that it would not continue to track consumer use once a given consumer had turned off that feature.

92. By continuing to track consumers who turned off these settings, Apple breached that implied contract.

93. Apple’s breach of this implied contract caused damages to Plaintiff and similarly situated class members, including nominal damages and other damages to be determined at trial.

FIFTH CAUSE OF ACTION

Unjust Enrichment (On Behalf of Plaintiff and the Class)

94. Plaintiff incorporates by reference all allegations in this Complaint and restates them as if fully set forth herein. This claim is pled in the alternative to the contract-based claim.

95. Plaintiff and class members conferred a tangible and material economic benefit upon Defendant. Despite branding itself as a company that respects privacy and offers consumers the ability to prevent data tracking, Defendant nonetheless collected Plaintiff’s and the class members’ private data.

96. Defendant was unjustly enriched thereby, using Plaintiff and the class members’ data to enhance advertising revenue and its products.

97. Defendant’s retention of the benefit conferred upon them by Plaintiff and the Class would be unjust and inequitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, prays for relief and judgment against Defendant as follows:

- A. certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiff as representatives of the Class, and designating Plaintiff's counsel as Class Counsel;
- B. declaring that Defendant's conduct violates the laws referenced herein;
- C. finding in favor of Plaintiff and the Class on all counts asserted herein;
- D. awarding Plaintiff and the Class compensatory damages and actual damages, trebled, in an amount exceeding \$5,000,000, to be determined by proof;
- E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;
- F. awarding Plaintiff and the Class punitive damages;
- G. awarding Plaintiff and the Class civil penalties;
- H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;
- I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;
- J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;
- K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;
- L. awarding pre-judgment and post-judgment interest; and
- M. granting any other relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: January 27, 2023

/s/ Benjamin J. Eichel

BONI, ZACK & SNYDER LLC

Michael J. Boni (Pa. Bar. No. 52983)

Joshua D. Snyder (Pa. Bar. No. 88657)

Benjamin J. Eichel (Pa. Bar. No. 307078)

15 St. Asaphs Road

Bala Cynwyd, PA 19004

Telephone: (610) 822-0200

Facsimile: (610) 822-0206

E-Mail: mboni@bonizack.com

jsnyder@bonizack.com

beichel@bonizack.com

BURSOR & FISHER, P.A.

Philip L. Fraietta (*pro hac vice* forthcoming)

Matthew A. Girardi (*pro hac vice* forthcoming)

Julian C. Diamond (*pro hac vice* forthcoming)

888 Seventh Avenue

New York, NY 10019

Telephone: (646) 837-7150

Facsimile: (212) 989-9163

E-Mail: pfraietta@bursor.com

mgirardi@bursor.com

jdiamond@bursor.com

Attorneys for Plaintiffs